На правах рукописи

Гончаров Максим Максимович

Комплексное управление рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности

Специальность: 05.13.01 – Системный анализ, управление и обработка информации (промышленность)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Тверь 2014

Работа выполнена в филиале федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Национальный исследовательский университет «МЭИ» в г. Смоленске на кафедре «Вычислительная техника»

Научный руководитель: **Борисов Вадим Владимирович** – доктор технических наук, профессор, профессор кафедры «Вычислительная техника» филиала МЭИ в г. Смоленске

Официальные оппоненты:
Бутусов Олег Борисович – доктор физико-математических наук, профессор, заведующий кафедрой «Прикладная математика» Московского государственного машиностроительного университета (МАМИ),

Мищенко Владимир Ильич – доктор технических наук, профессор, профессор кафедры естественнонаучных дисциплин Военной академии войсковой ПВО ВС РФ им. Маршала Советского Союза А.М. Василевского

Ведущая организация: ФГБОУ ВПО «Российский химико-технологический университет им. Д.И. Менделеева», г. Москва

Защита состоится «__» _____ 2014 г. в __ часов на заседании диссертационного совета Д 212.262.04 при Тверском государственном техническом университете по адресу: 170026, г. Тверь, наб. Афанасия Никитина, 22.

С диссертацией можно ознакомиться в библиотеке Тверского государственного технического университета.

Отзывы в двух экземплярах, заверенные печатью организации, просим направлять по адресу: 170026, г. Тверь, наб. Афанасия Никитина, 22, Ученый совет Тверского государственного технического университета

Автореферат разослан «___»_____2014 г.

Ученый секретарь диссертационного совета Д 212.262.04
д.ф.-м.н., проф. С.М. Дзюба

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Нефтеперерабатывающие предприятия относятся к отрасли, которая априори не является безопасной. Эффективность процессов предприятий нефтеперерабатывающей промышленности (ПНПП) во многом обусловлена своевременной и качественной передачей и обработкой данных в системах обработки информации (СОИ) этих предприятий. Причем, специфика этих информационных процессов, а также информационных ресурсов, формируемых и используемых в рамках этих процессов, заключается в том, что их нарушение, как правило, приводит к остановке производственных процессов нефтеперерабатывающего предприятия, что в итоге влечет существенные убытки. Кроме того, пристальное внимание к данной задаче объясняется тем, что оценка и управление рисками необходимы при контроле и мониторинге защищенности систем обработки информации и требуют обработки большого объема данных в условиях дефицита времени.

В настоящее время наблюдается тенденция на интеграцию СОИ разнопрофильных ПНПП в единое информационное пространство. Для этого необходимо обеспечить эффективную периметральную защиту СОИ каждого ПНПП, что невозможно без эффективного управления рисками в СОИ ПНПП с поддержанием заданного уровня их безопасности.

Активно развиваются методы оценки и непрерывного управления рисками информационной безопасности. Во взаимосвязи с современными моделями управления системами обработки информации, системами управления информационной безопасности, мониторинга и анализа защищенности данные методы позволяют наиболее быстро и эффективно строить и развивать систему защиты информации предприятий. Особая роль при управлении рисками в СОИ ПНПП отводится автоматизированному учету угроз, связанных с появлением новых уязвимостей в СОИ, агрегированию данных из различных источников, оперативному формированию отчетов о состоянии защищенности СОИ, определению набора приоритетных контрмер с учетом возможных рисков, а также прогнозированию рисков информационной безопасности.

Вместе с тем в сфере управления рисками в системах обработки информации применительно к предприятиям нефтеперерабатывающей промышленности существует целый ряд проблем.

Управление рисками в СОИ ПНПП осуществляется в условиях комплексного воздействия рискообразующих факторов, неопределенности системных и внешних параметров. Существующие трактовки рисков не позволяют в полной мере описать комплексный характер их воздействия на отдельные аспекты информационной безопасности, на информационные ресурсы и на систему обработки информации ПНПП в целом, а также учесть возможные негативные последствия и способы воздействия на них. Созданию и программной реализации методов и моделей управления рисками посвящены работы таких исследователей, как С.В. Артюхов, О.А. Базюкина, В.Ю. Королев, А.А. Кудрявцев, В.Е. Бенинг, С.Я. Шоргин, N. Crockford, Morgan, Granger и др.

Вместе с тем специфика задач управления рисками в СОИ ПНПП требует, во-первых, реализации комплексного подхода к управлению ими, во-вторых, создания методов, алгоритмов и программных средств управления рисками, учитывающих различные условия неопределенности. Среди подходов к учету неопределенности различного типа при управлении рисками в СОИ ПНПП обоснованным является использование методов нечеткого моделирования, предложенных в работах А.Е. Алтунина, И.З. Батыршина, А.Н. Борисова, Л.С. Берштейна, С.Я. Коровина, О.А. Крумберга, А.Н. Мелихова, С.А. Орловского, М.В. Семухина, В.Б. Силова, J.C. Bezdek, R. Bellman, J.L. Castro, D. Dubuis, A. Kaufmann, H. Larsen, E. Mamdani, H. Prade, M. Sugeno, T. Takagi, T. Terano, Y. Tsukamoto, R. Yager и др., а нечетких и гибридных нечетких моделей, существенный вклад в создание которых внесли Л.Г. Комарцова, А.С. Федулов, А.В. Язенин, Н.Г. Ярушкина, R. Fuller, Y. Hayashi, D.J. Hunt, J.-S.R. Jang, J.M. Keller, B. Kosko, R. Krishnapuram, E.T. Lee, H.-M. Lee, S.C. Lee, J.M. Mendel, S. Mitra, S. Pal, W. Pedrycz, D. Rutkowski, L. Rutkowski, C.-T. Sun, L.X. Wang и др.

Однако для реализации основных этапов комплексного управления рисками требуется создание гибридных нечетких моделей, и основанных на них алгоритмов, с одной стороны учитывающих специфику системных и внешних факторов СОИ ПНПП, а с другой, позволяющих осуществить их представление, алгоритмическую и программную реализацию в рамках единого метода.

Исследования в области создания программных средств, реализующих интеллектуальные методы и модели, основываются на работах отечественных ученых Д.А. Поспелова, А.Н. Аверкина, А.А. Башлыкова, В.Н. Вагина, В.В. Емельянова, А.П. Еремеева, Н.Г. Загоруйко, О.П. Кузнецова, В.М. Курейчика, О.И. Ларичева, А.С. Нариньяни, Г.С. Осипова, Б.В. Палюха, А.Б. Петровского, Г.С. Плесневича, В.Э. Попова, Г.В. Рыбиной, Н.А. Семенова, В.А. Смирнова, В.Б. Тарасова, В.В. Троицкого, В.К. Финна, И.Б. Фоминых, В.Ф. Хорошевского и др.; зарубежных ученых J. Allen, C. Demetresku, R. Detcher, A. Gereviny, G. Italiano, A. Krokhin, I. Meiri, L. Schubert, T. Saaty, T. Van Allen и др.

В то же время, в недостаточной степени развиты программные средства управления рисками в СОИ ПНПП на основе гибридных нечетких моделей, позволяющих учесть комплексное воздействие рискообразующих факторов, неопределенность системных и внешних параметров на всех этапах управления этими рисками.

Таким образом, задача исследования и разработки методики и алгоритмов комплексного управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности на основе нечетких гибридных моделей, является актуальной и практически значимой.

Целью исследования является повышение эффективности управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности за счет использования методики, алгоритмов и программных средств комплексного управления рисками в этих системах на основе гибридных нечетких моделей.

Объектом исследования является система обработки информации предприятия нефтеперерабатывающей промышленности.

Предметом исследования являются процессы управления рисками в системе обработки информации предприятия нефтеперерабатывающей промышленности.

Методы исследования. Проведенные теоретические и прикладные исследования базируются на методах системного анализа, теории принятия решений, теории нечетких множеств, нечеткой логики и нечеткого моделирования, а также на методах объектно-ориентированного проектирования и программирования.

Научной задачей исследования является разработка и исследование методики и алгоритмов комплексного управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности на основе гибридных нечетких моделей.

Для решения научной задачи исследования должны быть выполнены следующие **задачи.**

1. Исследование задач, методик и моделей управления рисками в СОИ ПНПП.

2. Разработка методики комплексного управления рисками в СОИ ПНПП, основанного на гибридных нечетких моделях.

3. Создание методики формирования информационных ресурсов СОИ ПНПП.

4. Разработка гибридной нечеткой модели оценки рисков СОИ ПНПП и способа ее построения.

5. Разработка алгоритмов оценки, прогнозирования рисков и выбора мероприятий по обеспечению безопасности СОИ ПНПП для решения основных задач комплексного управления рисками.

6. Создание программных средств для комплексного управления рисками в СОИ ПНПП, реализующих предлагаемую методику и алгоритмы.

7. Разработка методики, оценка эффективности управления рисками на основе разрабатываемых программных средств и выработка рекомендаций по их использованию в СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ».

Научная новизна работы заключается в следующем.

1. Создана методика комплексного управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности, основанная на гибридной нечеткой модели, позволяющая оперативно решать задачи анализа, сопоставления, прогнозирования рисков и выбора мероприятий по обеспечению безопасности в этих системах в условиях неопределенности, комплексно учитывающая постоянные и кратковременно влияющие рискообразующие факторы на всех этапах управления этими рисками.

2. Предложена гибридная нечеткая модель оценки рисков СОИ ПНПП на основе нечетких когнитивных карт и нечетких автоматов, позволяющая учесть комплексное воздействие рискообразующих факторов, неопределенность системных и внешних параметров: во-первых, при оценке различных аспектов безопасности; во-вторых, при последующем обобщении результатов и получении отчета о состоянии безопасности системы в целом; в-третьих, при выборе мероприятий по обеспечению безопасности системы обработки информации; в-четвертых, при прогнозировании рисков в СОИ ПНПП.

3. Разработаны алгоритмы, реализующие основные этапы методики комплексного управления рисками в СОИ ПНПП. Предложен алгоритм оценки рис-

ков в СОИ ПНПП, обеспечивающий выполнение задач анализа и сопоставления рисков с учетом взаимосвязей между различными рискообразующими факторами, влияющими на уровни рисков. Разработан алгоритм выбора мероприятий по обеспечению безопасности СОИ ПНПП, позволяющий оценить эффективность применяемых политик безопасности и включенных в них мероприятий на основе их опосредованного влияния на уровни рисков СОИ ПНПП. Предложен алгоритм прогнозирования рисков в СОИ ПНПП, позволяющий учитывать различную степень влияния периодически возникающих в системе негативных факторов (угроз и уязвимостей) и выбираемых мероприятий на уровни рисков в СОИ ПНПП.

Практическую значимость работы составляют следующие результаты.

1. Предложена методика формирования информационных ресурсов СОИ ПНПП, позволяющая формализовать и автоматизировать решение задач: сбора и обобщения данных о процессах ПНПП; обоснования состава и структуры информационных ресурсов, определения их характеристик; построения модели доступа к информационным ресурсам в рамках конкретной СОИ.

2. Разработана структура программных средств и реализованы алгоритмы построения и использования гибридной нечеткой модели оценки рисков СОИ ПНПП.

3. Созданы программные средства управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности на основе разработанных методики, алгоритмов и моделей. Предложены рекомендации по использованию предложенных средств комплексного управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности.

На защиту выносятся

1. Методика комплексного управления рисками в СОИ ПНПП, основанная на гибридной нечеткой модели, обеспечивающий оценку, прогнозирование рисков и выбор мероприятий по обеспечению безопасности в этих системах.

2. Гибридная нечеткая модель оценки рисков в СОИ ПНПП на основе нечетких когнитивных карт и нечетких автоматов, позволяющая проводить анализ, сопоставление и прогнозирование рисков, а также выбор мероприятий по обеспечению безопасности в СОИ ПНПП.

3. Алгоритмы оценки, прогнозирования рисков и выбора мероприятий по обеспечению безопасности в СОИ ПНПП на основе разработанной гибридной нечеткой модели, реализующие основные этапы методики комплексного управления рисками в СОИ ПНПП.

4. Структура и алгоритмы программных средств комплексного управления рисками в СОИ ПНПП, основанные на предлагаемых методике и моделях.

Обоснованность научных результатов, выводов и рекомендаций, сформулированных в работе, определяется корректным применением методов исследования. **Достоверность** научных положений подтверждена соответствием теоретических положений и результатов экспериментов на основе компьютерного моделирования, сопоставлением полученных результатов с результатами, приведенными в научной литературе, а также итогами практического применения методики, алгоритмов и программных средств при комплексном управлении рисками СОИ ПНПП.

Реализация результатов работы. Разработанные программные средства используются в ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» для комплексного управления рисками в системе обработки информации. По результатам оценки рисков были выбраны и обоснованы мероприятия по обеспечению безопасности и постоянной работоспособности СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ». Теоретические и практические результаты работы использованы при разработке нечетких моделей оценки, прогнозирования и выбора мероприятий по обеспечению информационной безопасности сложных организационно-технических систем были использованы в рамках НИР:

«Исследование и разработка методов и моделей интеллектуального управления рисками в сложных организационно-технических системах», Минобрнауки России, договор № 1043110, № гос. рег. 01201067780, 2011–2013 г.г.

«Исследование и разработка методов, моделей и технологий интеллектуального анализа данных и поддержки принятия решений в топливно-энергетическом комплексе», выполненной при поддержке Минобрнауки России в рамках базовой части Госзадания «Проведение научно-исследовательских работ (фундаментальных научных исследований, прикладных научных исследований и экспериментальных разработок)», Минобрнауки России, договор № 1013140, № гос. рег. 01201458416, 2014–2016 г.г.

Результаты работы используются в учебном процессе филиала ФГБОУ ВПО «НИУ «МЭИ» в г. Смоленске, что подтверждено соответствующими актами о внедрении.

Апробация результатов работы. Основные результаты работы докладывались и обсуждались на конференциях: III Межвузовская научно-практическая студенческая конференция «Молодежь. Наука. Инновации» (Смоленск, 2010); IV International Research and Practice Conference «Science and Education» (Munich, Germany, 2013); Межвузовская конференция «Вопросы информатизации учебного процесса, научных исследований и управления» (Смоленск, 2013).

Публикации. По результатам диссертационной работы опубликовано 9 работ, в том числе 3 статьи в изданиях из перечня ВАК. Результаты диссертации также отражены в 1 отчете о НИР.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы, включающего 114 наименований. Диссертация содержит 144 страниц машинописного текста, 21 рисунок, 5 таблиц, 1 приложение.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении диссертации обоснована актуальность темы исследований, определены цель и научная задача диссертационной работы, сформулированы научная новизна и практическая значимость результатов исследований.

В первой главе выполнен анализ задач, методов и моделей управления рисками в системах обработки информации предприятий нефтеперерабатывающей промышленности. Рассмотрены существующие программные средства анализа и рисками информационной безопасности.

Определены характеристики и особенности системы обработки информа-

ции с учетом специфики предприятий нефтеперерабатывающей промышленности, к которым, прежде всего, относятся следующие:

- пространственная распределенность и сложная структура системы;
- высокая важность информационных ресурсов СОИ ПНПП;
- нарушение информационных процессов СОИ приводит к высоким убыткам ПНПП, устранение неполадок должно проходить в короткие сроки;
- предотвращение потерь в СОИ ПНПП более эффективно, чем устранение последствий нарушений безопасности;
- анализ и управление рисками СОИ ПНПП традиционными методами требует обработки избыточного объема данных в условиях дефицита времени.

Рассмотрены основные процессы в ПНПП, такие как:

- производственные процессы, направленные на создание определенных продуктов или услуг;
- управляющие процессы, позволяющие управлять предприятием и обеспечивающие его конкурентоспособность и развитие;
- поддерживающие процессы или процессы обеспечения, поддерживающие инфраструктуру и работоспособность предприятия.

Уточнено понятие и сформулированы требования для представления информационных ресурсов в СОИ ПНПП, представляющих собой совокупность данных, организованных для эффективной реализации производственных и управляющих процессов ПНПП.

Рассмотрено определение политики информационной безопасности, также рассмотрены цели и задачи создания политики безопасности. Проведен анализ различных определений риска. Выполнен анализ и представлена классификация информационных угроз и уязвимостей в СОИ ПНПП. Приведены основные способы анализа и выявления угроз информационной безопасности. Проведен анализ существующих подходов к снижению уровней рисков. Рассмотрены методы управления рисками в СОИ ПНПП, приведены основные этапы процесса по обеспечению информационной безопасности. Выполнен обзор мероприятий по снижению уровней рисков информационной безопасности.

Выполнен анализ и обосновано совместное использование нечетких автоматов и нечетких когнитивных карт для реализации различных задач комплексного управления рисками, с одной стороны, учитывающих специфику системных и внешних факторов и условия неопределенности в СОИ ПНПП, а с другой, позволяющих осуществить их представление, алгоритмическую и программную реализацию в рамках единой методики.

Рассмотрены программные средства и платформы для управления рисками. Сформулированы требования к разрабатываемым методики и алгоритмам комплексного управления рисками в СОИ ПНПП. Выдвинуты требования к разрабатываемым программным средствам.

Во второй главе описана предлагаемая методика комплексного управления рисками в СОИ ПНПП. Уточнены понятия рисков для отдельных аспектов информационной безопасности, информационных ресурсов и СОИ ПНПП в целом. Предложена методика формирования информационных ресурсов СОИ ПНПП. Разрабо-

тана гибридная нечеткая модель оценки рисков в СОИ ПНПП на основе нечетких когнитивных карт и нечетких автоматов, а также способ построения этой модели.

Под риском информационной безопасности понимается вероятность (возможность) наступления неблагоприятного события по причине реализации угроз, направленных на уязвимости информационных ресурсов с учетом возможных негативных последствий. Для отдельного аспекта информационной безопасности, на который влияет одна угроза, направленная на одну уязвимость, риск оценивается следующим образом:

$$R_i = P_{Угрозы} * P_{Уязвимости} * C_{Ущерба},$$

где $P_{Угрозы}, P_{Уязвимости}, C_{Ущерба}$ – возможность угрозы, степень уязвимости, значение ущерба, соответственно; $*$ – операция для расчета R_i, выбираемая в зависимости характеристики, типа переменных, способа учета неопределенности.

Для отдельного информационного ресурса СОИ ПНПП, необходимо учитывать различные угрозы и уязвимости, сложным образом влияющие на значение риска этого информационного ресурса $R_{ИР}$. При этом для оценки $R_{ИР}$ можно воспользоваться нечеткой продукционной моделью с адаптацией операций над нечеткими множествами следующего вида:

Π_1: **ЕСЛИ** x_1 есть H_1 **И** … **И** x_q есть H_q,
ТО y есть $(H_1\ \theta_1^1\ H_{ИР})\ \vartheta_l^1$, …, $\vartheta_l^1\ (H_q\ \theta_q^1\ H_{ИР})$,

…

Π_i: **ЕСЛИ** x_1 есть M_1 **И** … **И** x_q есть L_q,
ТО y есть $(M_1\ \theta_1^i\ M_{ИР})\ \vartheta_l^i$,…, $\vartheta_l^i\ (L_q\ \theta_q^i\ M_{ИР})$,

…

Π_n: **ЕСЛИ** x_1 есть L_1 **И** … **И** x_q есть L_q,
ТО y есть $(L_1\ \theta_1^n\ L_{ИР})\ \vartheta_l^n$, …, $\vartheta_l^n\ (L_q\ \theta_q^n\ L_{ИР})$.

где x_1, …, x_q – входные переменные для этой модели, характеризующие значения рисков для отдельных аспектов информационной безопасности; y – выходная переменная; $\{L_j, M_j, H_j\}$ – нечеткие множества, характеризующие степень риска j-му аспекту безопасности R_j, и заданные своими функциями принадлежности $L_j = \{(\mu_{L_j}(x), x) \mid x \in X_j\}$, $M_j = \{(\mu_{M_j}(x), x) \mid x \in X_j\}$, $H_j = \{(\mu_{H_j}(x), x) \mid x \in X_j\}$, $j = 1, \ldots, q$; $\{L_{ИР}, M_{ИР}, H_{ИР}\}$ – нечеткие множества, характеризующие степень риска относительно информационного ресурса $R_{ИР}$, и заданные своими функциями принадлежности $L_{ИР} = \{(\mu_{L_{ИР}}(y), y) \mid y \in Y\}$, $M_{ИР} = \{(\mu_{M_{ИР}}(y), y) \mid y \in Y\}$, $H_{ИР} = \{(\mu_{H_{ИР}}(y), y) \mid y \in Y\}$; $\theta_1^1, \ldots, \theta_q^1, \ldots, \theta_1^n, \ldots, \theta_q^n$ – операции свертки значения риска информационному ресурсу со значением риска отдельному аспекту безопасности, выбираемые в зависимости от уровня их совместимости; ϑ_l^i – операция комбинирования результатов сверток значений риска информационному ресурсу со значениями риска по отдельным аспектам безопасности в i-м правиле ($i = 1, \ldots, n$), выбираемая из соответствующей совокупности операций парных сверток $\theta_1^i \ldots, \theta_q^i$ и характеризующая нижний уровень их согласованности.

Подобным образом оцениваются и риски СОИ ПНПП в целом $R_{СОИ}$, которые формируется на основе рисков информационных ресурсов с учетом возможного

ущерба. Этот подход целесообразно использовать для получения агрегированной оценки рисков и реализовывать с использованием нечетких когнитивных карт.

На рис. 1 представлена схема предлагаемой методики комплексного управления рисками в СОИ ПНПП. Методика комплексного управления рисками СОИ ПНПП основана на гибридной нечеткой модели, алгоритмах оценки и прогнозирования рисков СОИ ПНПП и алгоритме выбора мероприятий. Разработанная методика обеспечивает реализацию этапов процесса комплексного управления рисками СОИ ПНПП, позволяет рассматривать различные риски и обеспечивает одновременный учет рискообразующих факторов различной природы.

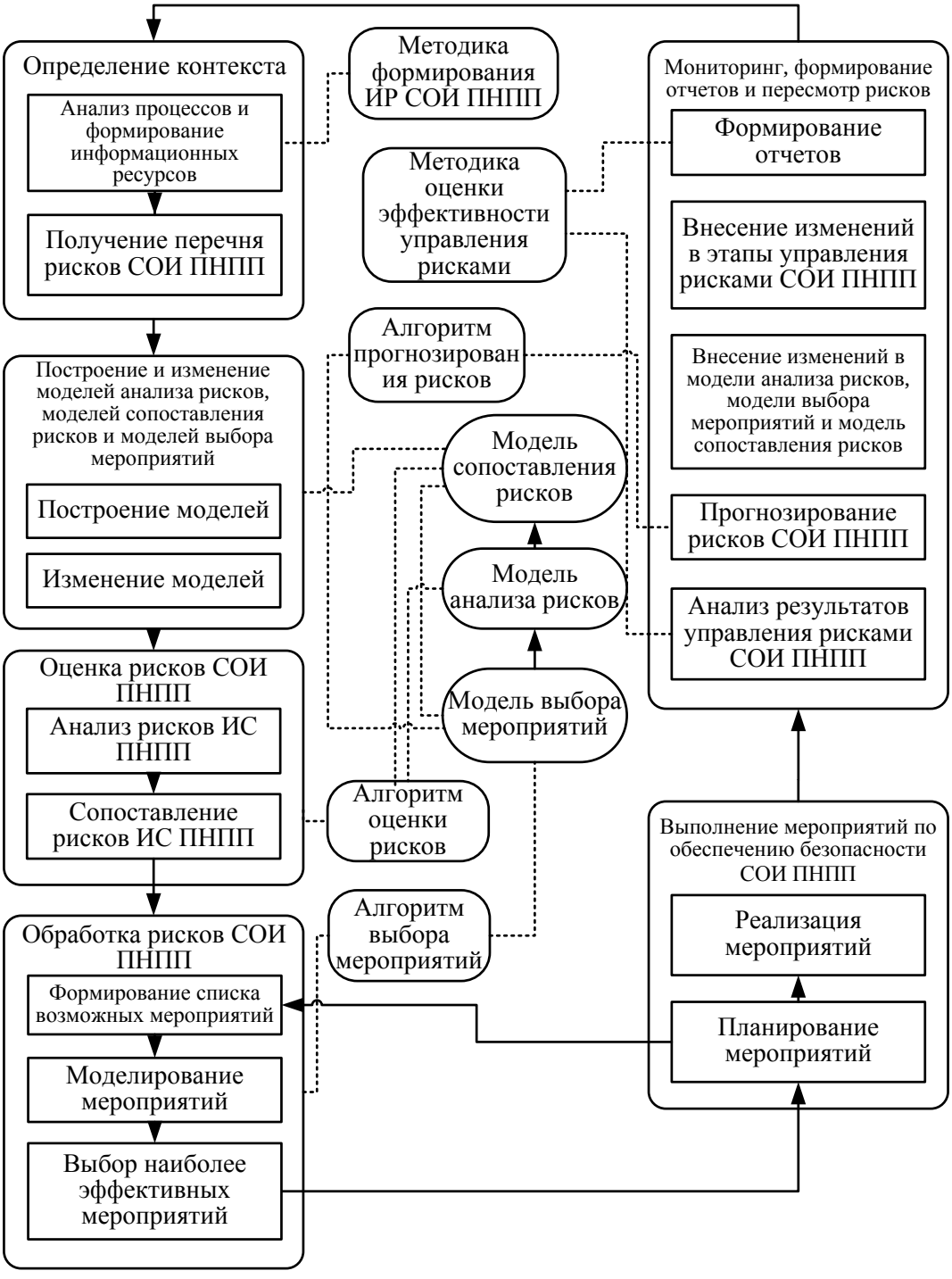

Рис. 1. Схема метода комплексного управления рисками в СОИ ПНПП

Основными этапами методики являются следующие.

Этап 1. Определение контекста (результаты этапа – перечень информационных ресурсов СОИ ПНПП и их характеристик, перечень рисков, угроз, уязвимостей и ущерба).

Этап 2. Построение и изменение моделей анализа рисков, моделей сопоставления рисков и моделей выбора мероприятий (результаты этапа – построенная гибридная нечеткая модель оценки рисков в СОИ ПНПП)

Этап 3. Оценка рисков (результаты этапа – уровни рисков и их сопоставление с целевыми уровнями рисков в СОИ ПНПП).

Этап 4. Обработка рисков (результаты этапа – перечень наиболее эффективных мероприятий и политик безопасности).

Этап 5. Выполнение мероприятий (результаты этапа – отчет о выполнении мероприятий за определенный период).

Этап 6. Мониторинг, формирование отчетов и пересмотр рисков (результаты этапа – отчет о результатах комплексного управления рисками за определенный период и управленческие решения о дальнейшем управлении рисками в СОИ ПНПП).

Для решения 1-го этапа предлагаемой методики создана методика формирования информационных ресурсов СОИ ПНПП, позволяющая формализовать и автоматизировать решение задач: сбора и обобщения данных о производственных и управляющих процессах ПНПП; обоснования состава и структуры информационных ресурсов, определения их характеристик; построения модели доступа к информационным ресурсам в рамках конкретной СОИ.

Предложена гибридная нечеткая модель оценки рисков СОИ ПНПП. Данная гибридная модель включает в себя: во-первых, нечеткий автомат сопоставления уровней рисков $НА_с$; во-вторых, совокупность нечетких когнитивных карт $НКК_1, НКК_2, ..., НКК_i$ для анализа отдельных рисков; в третьих, набор нечетких автоматов для выбора мероприятий $НА_{м1}, НА_{м2}, ..., НА_{мj}, ..., НА_{мт}$ для оценки воздействия на риски.

На рис. 2 представлена обобщенная структура гибридной нечеткой модели оценки рисков СОИ ПНПП. Предложенный способ построения гибридной нечеткой модели оценки рисков в СОИ ПНПП включает в себя три процедуры. Сначала выполняется построение нечетких когнитивных карт для анализа рисков относительно каждого аспекта безопасности ИР. Затем выполняется построение нечеткого автомата для сопоставления уровней рисков СОИ ПНПП. После анализа и сопоставления рисков принимается решение о создании и применении политики безопасности, состоящей из определенного набора мероприятий. Для этого выполняется построение нечетких автоматов для выбора мероприятий.

При построении нечеткой когнитивной карты $НКК_i$ выделяется: ДК – дестабилизирующие концепты, отображающие угрозы; ВК – внутренние концепты, представляющие собой группы объектов либо параметры, описывающие уязвимости и средства защиты; ЦК – целевые концепты, описывающие различные негативные последствия (ущерб), возникающие в результате воздействия дестабилизирующие концепты; КР – концепты риска, описывающие итоговое значение риска.

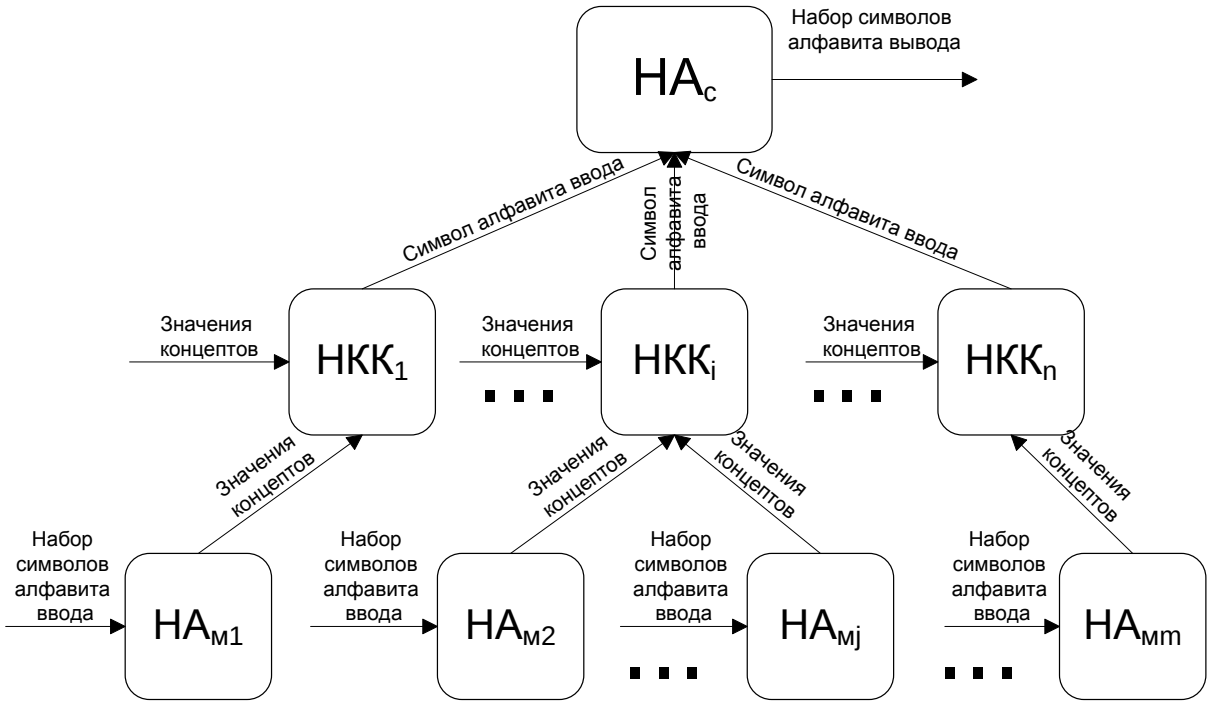

Рис. 2. Обобщенная структура гибридной нечеткой модели оценки рисков СОИ ПНПП

Предложены следующие выражения для анализа рисков с использованием нечетких когнитивных карт, учитывающих специфику СОИ ПНПП:

- для оценки влияния дестабилизирующих факторов на уровни рисков:

$$G_{KPi} = \bigoplus_{j=1}^{n}{}_1(W_{ДКjKPi} * G_{ДКj}) = \max(W_{ДК1KPi} * G_{ДК1}, W_{ДК2KPi} * G_{ДК2}, ..., W_{ДКjKPi} * G_{ДКj}).$$

где $\oplus_1$ – операция агрегирования воздействий дестабилизирующих факторов;

- для оценки влияния целевых концептов на концепты риска:

$$G_{KPi}(t+1) = \bigotimes_{j=1}^{n}{}_2(G_{KPi}(t), \max(W_{ЦК1KPi} * G_{ЦК1}(t), W_{ЦК2KPi} * G_{ЦК2}(t), ..., W_{ЦКjKPi} * G_{ЦКj}(t))) =$$

$$= \min(G_{KPi}(t), \max(W_{ЦК1KPi} * G_{ЦК1}(t), W_{ЦК2KPi} * G_{ЦК2}(t), ..., W_{ЦКjKPi} * G_{ЦКj}(t))).$$

- для оценки динамики изменения значения концепта:

$$G_i(t+1) = G_i(t) + \sum_{j=1}^{n}((G_j(t) - G_j(t))W_{ji}).$$

При учете угроз и уязвимостей, сложным образом влияющих на значение риска информационного ресурса $R_{ИР}$ и если значения вероятностей (возможностей) угроз и уязвимостей можно получить только в качественном виде, предлагается в рамках НКК использовать рассмотренную выше нечеткую продукционную модель.

Нечеткий автомат для сопоставления уровней рисков СОИ ПНПП, а также нечеткие автоматы для выбора мероприятий представляются в следующем виде:

$$\tilde{F} = < A, Q, B, \tilde{R}, \delta, \omega, F_1, F_2 >$$

где: $A = \{a_1, ..., a_m\}$ – конечный алфавит ввода, $Q = \{q_1, ..., q_n\}$ – набор состояний, $B = \{b_1, ..., b_k\}$ – конечный алфавит вывода, q_0 – нечеткое начальное состояние,

$\delta: \sum \times Q \times [0,1] \to Q$ – карта нечетких переходов, $\omega: Q \to B$ – функция вывода, $F_1: [0,1] \times [0,1] \to [0,1]$ – функция принадлежности состояния, $F_2: [0,1]^* \to [0,1]$ – функция мульти-принадлежности (используется в тех ситуациях, если несколько активных состояний переходят в одно и то же состояние и выводит общее значение принадлежности для расчета нового активного состояния).

Предлагаемая гибридная нечеткая модель оценки рисков позволяет учесть комплексное воздействие рискообразующих факторов, неопределенность системных и внешних параметров при решении задач анализа и сопоставления и рисков, а также при выборе мероприятий по обеспечению безопасности СОИ ПНПП.

В третьей главе разработаны алгоритмы оценки, прогнозирования рисков и выбора мероприятий по обеспечению безопасности СОИ ПНПП для решения основных задач комплексного управления рисками.

Алгоритм оценки рисков в СОИ ПНПП обеспечивает выполнение задач: анализа рисков с учетом взаимосвязей между различными рискообразующими факторами, непосредственно и опосредованно влияющими на уровни рисков для каждого аспекта информационной безопасности системы; задач сопоставления различных уровней этих рисков по всем аспектам информационной безопасности с последующем обобщением результатов этого анализа (рис. 3).

Алгоритм выбора мероприятий по обеспечению безопасности СОИ ПНПП позволяет оценить эффективность применяемых политик безопасности и включенных в них мероприятий на основе их опосредованного влияния на уровни рисков (рис. 4).

Алгоритм прогнозирования рисков в СОИ ПНПП позволяет учитывать различную степень влияния периодически возникающих в системе негативных факторов и выбираемых мероприятий на уровни рисков в СОИ ПНПП (рис. 5).

Рис. 3. Схема алгоритма оценки рисков

Рис. 4. Схема алгоритма выбора мероприятий

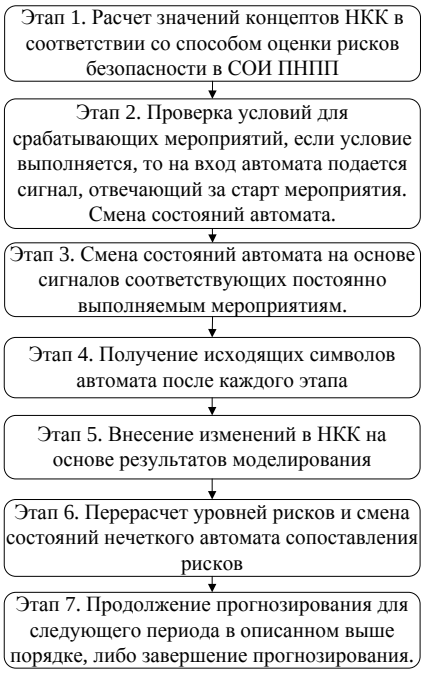

Рис. 5. Схема алгоритма прогнозирования рисков

В четвертой главе описаны разработанные программные средства управления рисками в СОИ ПНПП на основе предложенных методики, алгоритмов и моделей. Предложена методика, выполнена оценка эффективности и выработаны рекомендации по комплексному управлению рисками в СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» на основе разработанных программных средств.

В таблице 1 представлены результаты проведения мероприятий по результатам аудита СОИ «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» с помощью предложенной методики управления рисками.

В качестве показателя оценки эффективности комплексного управления рисками СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» с использованием разработанных программных средств выбран коэффициент возврата инвестиций, рассчитываемый для отдельно взятых мероприятий и политик безопасности. При использовании разработанных программных средств в течение 10 мес. при условии обеспечения требуемого уровня риска возврат инвестиций в ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» составил сумму 5255 тыс. рублей.

Таблица 1 – Изменение уровней рисков после выполнения мероприятий в рамках управления рисками СОИ «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ»

Риски	**Уровень до внедрения**	**Уровень после внедрения**	**Выполненные мероприятия**
Потеря отчетности и документов	Ниже среднего (36%)	Низкий (17%)	Внедрение систем резервирования информации
Потеря показателей датчиков реального времени	Ниже среднего (21%)	Низкий (17%)	
Остановка производственных процессов на удаленных участках производства	Низкий (19%)	Низкий (3%)	Резервирование каналов связи с удаленными участками производства
Остановка управляющих процессов в здании управления	Низкий (13%)	Низкий (4%)	Внедрение систем резервирования электропитания
Утечка конфиденциальных данных по каналам связи	Низкий (11%)	Низкий (6%)	Обновление оборудования зашифрованных VPN-каналов
Проникновение вредоносного ПО на ПК в здании управления	Средний (49%)	Низкий (17%)	Внедрение корпоративного антивируса, введение политики доступа к файловым хранилищам
Проникновение вредоносного ПО в файловые хранилища	Ниже среднего (28%)	Низкий (15%)	
Проникновение вредоносного ПО на АРМ на удаленных участках производства	Высокий (83%)	Низкий (19%)	
Утечка конфиденциальных данных	Ниже среднего (23%)	Низкий (11%)	Введение политики использования почтовых ящиков на внутреннем домене smolneft.ru
Спам	Низкий (15%)	Низкий (7%)	
Проникновение вредоносного ПО через почту	Низкий (13%)	Низкий (3%)	

В результате сравнительной оценки оперативности управления рисками при использовании известных и разработанных программных средств по критерию количества необходимых операций, которые позволяют сделать вывод о том, что в средне- и долгосрочной перспективе оперативность управления рисками в СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» возрастает в среднем на величину до 50% (рис. 6).

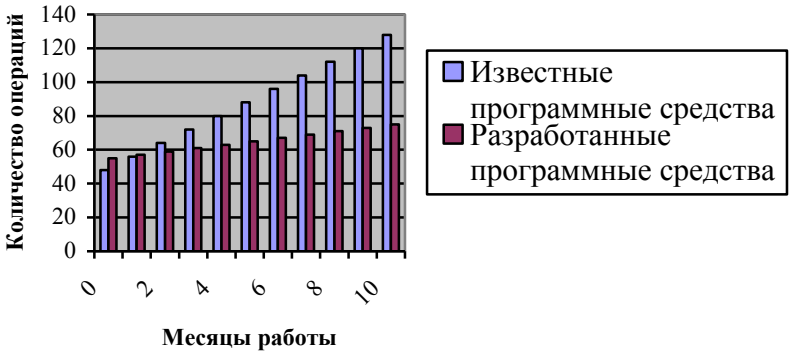

Рис. 6 – Число операций, затраченных на управление рисками

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате проведенных исследований решена научная задача разработки и исследования методики и алгоритмов комплексного управления рисками систем обработки информации предприятий нефтеперерабатывающей промышленности.

Основными результатами работы являются следующие.

1. Разработана методика комплексного управления рисками в СОИ ПНПП, основанная на гибридных нечетких моделях, обеспечивающая оценку, прогнозирование рисков и выбор мероприятий по обеспечению информационной безопасности в этих системах.

2. Создана методика формирования информационных ресурсов СОИ ПНПП для формализации и автоматизации: сбора и обобщения данных о процессах ПНПП; обоснования состава и структуры информационных ресурсов, определения их характеристик; построения модели доступа к информационным ресурсам в рамках конкретной СОИ.

3. Создана гибридная нечеткая модель оценки рисков СОИ ПНПП на основе нечетких когнитивных карт и нечетких автоматов, позволяющая проводить анализ, сопоставление и прогнозирование рисков, а также выбор мероприятий по обеспечению безопасности в этих системах.

4. Разработаны алгоритмы:

- оценки рисков в СОИ ПНПП для решения задач: анализа рисков с учетом взаимосвязей между различными рискообразующими факторами, влияющими на уровни рисков для различных аспектов информационной безопасности системы; сопоставления различных уровней этих рисков по всем аспектам информационной безопасности с обобщением результатов анализа;
- выбора мероприятий по обеспечению безопасности СОИ ПНПП и оценки эффективности применяемых политик безопасности;
- прогнозирования рисков в СОИ ПНПП с учетом различной степени влияния

на уровни рисков негативных факторов и выбираемых мероприятий.

5. Разработаны программные средства управления рисками в СОИ ПНПП на основе предложенных методики, алгоритмов и моделей.

6. Предложена методика, выполнена оценка эффективности и выработаны рекомендации по комплексному управлению рисками в СОИ ОАО «НК «РОСНЕФТЬ» – СМОЛЕНСКНЕФТЕПРОДУКТ» на основе разработанных программных средств.

Результаты диссертации опубликованы в следующих работах

Публикации в изданиях, рекомендованных ВАК Минобрнауки РФ

1. Гончаров М.М. Модель и способ анализа рисков информационной безопасности компьютерных систем на основе гибридных нечетких моделей / М.М. Гончаров // Нейрокомпьютеры: разработка, применение. – 2012, – №5. – С. 9–15.

2. Борисов В.В. Модель выбора мероприятий по обеспечению информационной безопасности на основе нечетких автоматов / В.В. Борисов, М.М. Гончаров // Программные продукты и системы. – 2014. – № 1. – С. 25–29.

3. Гончаров М.М. Гибридная нечеткая модель управления рисками систем обработки информации / М.М. Гончаров // Научное обозрение. – 2014. – № 1. – С. 123–129.

Публикации в других изданиях

4. Гончаров М.М. Об актуальности внедрения анализа рисков информационной безопасности / М.М. Гончаров // Сборник трудов по материалам III Межвузовской научно-практической студенческой конференции «Молодежь. Наука. Инновации». – 2010. – С. 137–139.

5. Гончаров М.М. Применение нечеткой логики при оценке рисков информационной безопасности / М.М. Гончаров // Сборник трудов по материалам III Межвузовской научно-практической студенческой конференции «Молодежь. Наука. Инновации». – 2010. – С. 85–88.

6. Гончаров М.М. Модель и способ выбора мероприятий по обеспечению информационной безопасности на основе нечетких автоматов / В.В. Борисов, М.М. Гончаров, И.И. Чукляев // Вестник Войсковой ПВО. – 2013, – № 10. – С. 156–163.

7. Goncharov M.M. Modeling of the information security events based on fuzzy automata / V.V. Borisov, M.M. Goncharov // IV International Research and Practice Conference «Science and Education», Munich, Germany, 2013, Vol. 1, – PP. 64–68.

8. Гончаров М.М. Нечеткая модель и способ обоснования и выбора контрмер по обеспечению безопасности информационных систем / М.М. Гончаров // Информационный бюллетень Смоленского регионального отделения АВН. – 2013. – №29. – С. 46–52.

9. Гончаров М.М. Гибридная нечеткая модель оценки рисков безопасности информационных систем / М.М. Гончаров // Сборник материалов Межвузовской конференции «Вопросы информатизации учебного процесса, научных исследований и управления». – 2013. – С. 17–22.

Подписано в печать .02.2014 г.
Формат 60x84$^{1}/_{16}$. Тираж 100 экз. Печ. л. 1,5
Отпечатано в издательском секторе МЭИ в г. Смоленске
214013 г. Смоленск, Энергетический проезд, 1